

Marktstudie:

„3rd Party Tools zur Überprüfung von Berechtigungen innerhalb von SAP“



Lukas Funk



mindsquare GmbH



Fachbereich Basis & Security

Einleitung

Die Notwendigkeit, ein Berechtigungstool einzuführen, ist in aller Regel getrieben von der Notwendigkeit eines effektiven und effizienten Identitäts- und Zugriffsmanagements in Verbindung mit der Umsetzung von Compliance-Anforderungen. [1]

Die ohnehin schon komplexen Anforderungen sind in den vergangenen Jahren noch einmal gestiegen. Große Unternehmen, die bis jetzt kein Berechtigungsmanagement einsetzen oder das Berechtigungsmanagement nicht mit der nötigen Konsequenz verwalten bekommen regelmäßig Probleme mit dem Wirtschaftsprüfer. Leider fehlt es vielen Unternehmen immer wieder an der Akzeptanz oder dem Know-how, um ein der Zeit gemäßes Berechtigungskonzept zu erstellen.

Die Wichtigkeit von „Segregation of Duty“ erschließt sich vielen Managern nicht. In jüngster Vergangenheit kann eine Vielzahl von handfesten Wirtschaftsskandalen festgestellt werden. Der regulatorische Druck steigt mit jedem weiteren Wirtschaftsskandal. Besonders hervorzuheben ist hierbei der Sarbanes-Oxley Act (SOX/SOA). Im Sarbanes-Oxley Act wird die Validierung von Berechtigungen von Unternehmen eingefordert. [2] Der SOX gilt für alle Unternehmen, deren Wertpapiere an einer der SEC Börsen gehandelt werden. Er ist daher auch für Unternehmungen außerhalb der USA relevant.

Unternehmen für die SOX eine Rolle spielt
Für Unternehmen, die ihre Wertpapiere (auch) an einer US-Börse notiert haben.
Für Unternehmen, die wesentliche Tochtergesellschaften ("significant subsidiary") einer an amerikanischen Börsen gehandelten Gesellschaft sind. [3]

Tabelle 1: Unternehmen, die SOX erfüllen müssen

Es gibt jedoch nicht nur den SOX als rechtliche Rahmenbedingung. Das COSO-Rahmen-Konzept, dass 1992 vom Committee of Sponsoring Organizations of the Treadway Commission (COSO) veröffentlicht wurde, definiert Bestandteile eines internen Kontrollsystems. (IKS) [4]

Weiterhin kann, als international weitgehend anerkanntes Regelwerk, der IT-Governance, CobiT genannt werden. CobiT ist ein Rahmenwerk zur regelkonformen Steuerung der IT in der Organisation. CobiT kann als Verbindung zwischen den unternehmensweiten Steuerungs-Frameworks (COSO) und den IT-spezifischen Normen (z. B. ITIL (IT Infrastructure Library), ISO 17799/27002) gesehen werden. [4] Dazu kommen noch weitere deutsche gesetzliche Richtlinien. Diese seien an dieser Stelle nur kurz erwähnt.

Gesetzliche Richtlinien in Deutschland
Grundsätze ordnungsgemäßer Buchführung (GoB)
Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS)
Handelsgesetzbuch (HGB)
Abgabeordnung und Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
Gesetz zur Kontrolle und Transparenz in Unternehmen (KonTraG) [4]

Tabelle 2: Deutsche Gesetzliche Richtlinien

Zu erkennen ist, dass die Berechtigungen immer mehr Aufwand in Anspruch nehmen. Es wird mehr und mehr Personal benötigt, um die wachsenden Anforderungen durch die verschiedenen rechtlichen Regelungen umzusetzen und zu überwachen. Hier kann es leicht zu einer Kostenexplosion kommen, wenn nicht auf die richtigen Tools zurückgegriffen wird. [5] Eine Marktstudie, die 3rd Party Berechtigungstools vergleicht, gibt es in dieser Form jedoch nicht auf dem Markt. In dieser Arbeit wird mit gezielten Fragen versucht, die Tools zu klassifizieren und zu bewerten.

Ziel der Arbeit ist ein Leitfaden, der jedem Unternehmer dabei helfen wird, das passende Tool für sein Unternehmen auszuwählen. Im ersten Teil wird auf die Vorbereitungen zur Studie eingegangen. Hier wird u.a. das Auswahlverfahren und die Kontaktkanäle der Fragen, um Teilnehmer für die Marktstudie zu gewinnen, erläutert. Im folgenden Teil wird auf den Aufbau der Studie eingegangen. Wie wurde die Umfrage strukturiert? Auf welchem Weg konnte ein Teilnehmer die Umfrage durchlaufen? Diese und weitere Fragen werden hier beantwortet. Es folgt die porträtartige Vorstellung von 3rd Party Toolherstellern. Hier wurde den Herstellern die Möglichkeit gegeben, ihr Tool kurz zu präsentieren. Als nächstes folgt ein Überblick über den Verlauf der Studie. Anschließend werden hier auch die Ergebnisse präsentiert. Als vorletztes folgt noch eine abschließende Empfehlung mit einem Fazit, bevor mit einem Ausblick geschlossen wird.

Aufbau der Umfrage

Die Umfrage konnte auf 2 verschiedenen Wegen durchlaufen werden. Abhängig von der Frage 2: „Haben Sie ein Berechtigungstool im Einsatz?“ wurde entweder der große Mittelteil der Studie eingeblendet oder Fragen, warum kein Tool eingesetzt wird. Danach wurden in beiden Fällen die Kontaktdaten erfragt.

Fragen
Wie würden Sie Ihr Aufgabenfeld am ehesten beschreiben?
Haben Sie ein Berechtigungstool im Einsatz?

Tabelle 3: Allgemein

Fragen
Welches Tool verwenden Sie?
Wie viel kostet Sie das Tool im Jahr?
Wie viele Dialogbenutzer verwalten Sie mit dem Tool?
Haben Sie Schulungen für das Werkzeug in Anspruch genommen?
Was ist Ihr größtes Problem mit der Lösung? (Freitext)
Was ist die beste Funktion der Lösung? (Freitext)
Wie lange Nutzen Sie das Tool schon?
Wie lange hat die Einführung gedauert?
Welche Schulnote würden Sie der Lösung insgesamt geben?

Tabelle 4: Allgemein Teil 2

Fragen
Wie gut fühlen Sie sich beim Rollenbau und Berechtigungsmanagement unterstützt?
Wie gut fühlen Sie sich bei der Auswertung kritischer Berechtigungen unterstützt?
Wie gut werden Sie bei der Auswertung von Funktionstrennungskonflikten unterstützt?
Wie unterstützt Sie das Tool bei einer zentralen Benutzerverwaltung (Identitymanagement)?
Wie unterstützt Sie das Tool beim Benutzermanagement?
Wie gut werden Sie bei der Erstellung von Dokumentation unterstützt?
Wie gut werden Sie bei der Fehleranalyse unterstützt?

Tabelle 5: Aufgaben und Funktion

Fragen
Ist das Werkzeug komplett innerhalb von SAP aufrufbar oder eine Anwendung außerhalb von SAP?
Können Rollen weiterhin im Standard bearbeiten werden (PFCG) oder wird das Tool benötigt?
Wie gut ist die Anwendungsdokumentation?
Wie bewerten Sie die Benutzerfreundlichkeit?
Wie bewerten Sie den Support?

Tabelle 6: Technik

Fragen
Wie viel würden Sie für ein Tool pro Jahr ausgeben wollen?
Wie viele Dialogbenutzer haben Sie?
Warum verwenden Sie kein Tool?

Tabelle 7: Kein Tool im Einsatz

Fragen
Bei welcher Firma arbeiten Sie?
Vorname
Nachname
E-Mail Adresse (hier erhalten Sie die fertige Marktstudie)

Tabelle 8: Allgemeine Angaben

Studienergebnisse

Überblick über die Ergebnisse

An der Marktstudie haben insgesamt 288 Unternehmen teilgenommen. Von diesen 288 Unternehmen haben 224 die Befragung komplett abgeschlossen und 64 Befragte haben vorher abgebrochen. Dies entspricht einem Wert von 78% für alle komplett abgeschlossenen und 22% für alle teilweise abgeschlossenen Fragebögen (Abbildung 2).

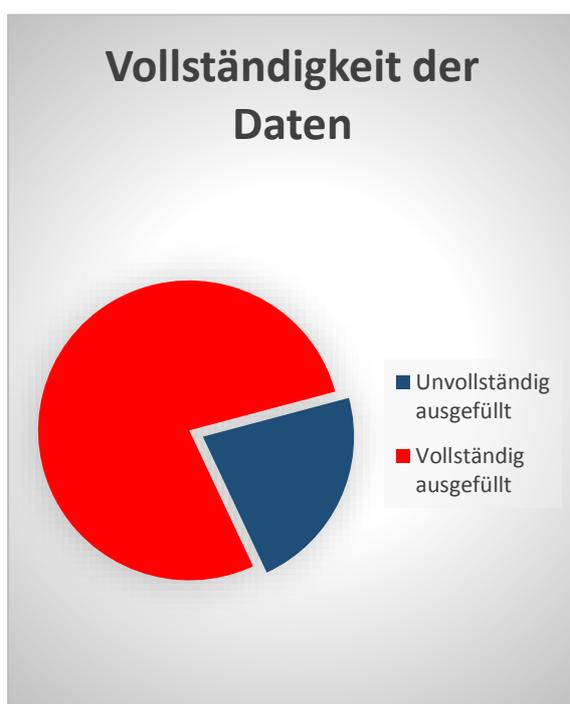


Abbildung 2: Vollständigkeit der Daten

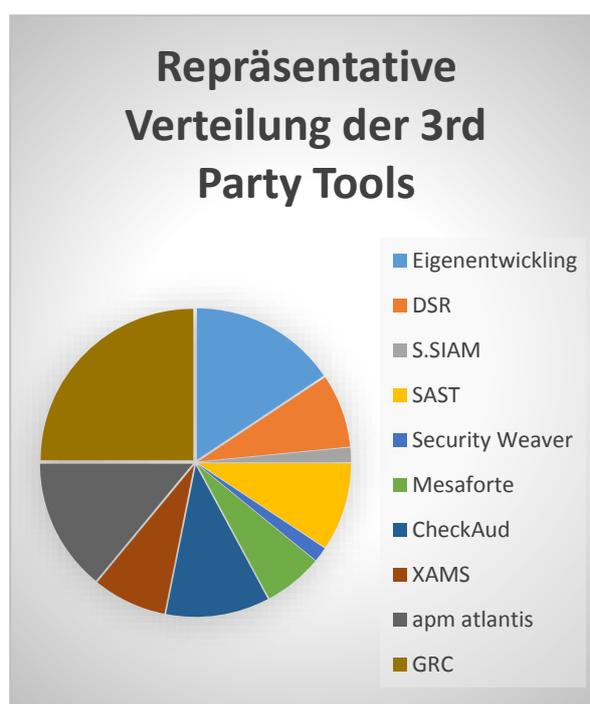


Abbildung 1: Repräsentative Verteilung der 3rd Party Tools

Es wurden viele unterschiedliche Tools bewertet. Neun Tools sind dabei besonders oft als eingesetztes Tool genannt worden.

Hierzu zählen DSR von nexQuent (8%), S.Siam von SIVIS (14%), SAST von akquinet (9%), Security Weaver vom gleichnamigen Hersteller (1%), Mesaforte von Wikima4 (4%), CheckAud von IBS Schreiber (7%), XAMS von XITING (8%), apm atlantis von relatime (9%) und GRC von SAP (16%). Weiterhin gibt es noch unterschiedliche Eigenentwicklungen (10%).

Kosten pro Jahr

Im Schnitt werden 9800 € pro Jahr für das eingesetzte 3rd Party Tool ausgegeben. Es ist sinnvoll nicht die komplette Suite zu kaufen sondern vorher zu überlegen, welche Teile der Suite genutzt werden sollen. Durch diese Überlegung kann viel Geld gespart werden.

Wie viel kostet Sie das Tool im Jahr?

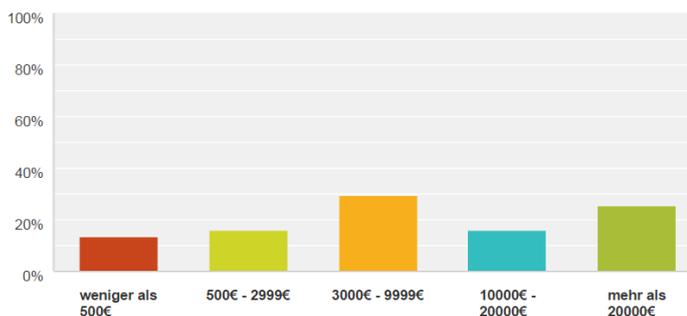


Abbildung 3: Kosten pro Jahr

13,41% der Teilnehmer zahlen weniger als 500 € im Jahr für den Einsatz eines 3rd Party Tools. 15,85% zahlen 500-2999 € und 29,27% zahlen 3000-9999 € im Jahr. 10000-20000€ werden von 15,85% der Teilnehmer im Jahr für den Einsatz von 3rd Party Software ausgegeben. Der Rest - 25,61% - zahlen mehr als 20000€ pro Jahr (Abbildung 3).

Tool	Kosten pro Jahr pro Tool in € (gerundet)						Anzahl Bewertungen
	<100	100-249	250-499	500-1499	1500-4999	>5000	
DSR	0%	40%	40%	20%	0%	0%	5
S.Siam	0%	0%	0%	0%	100%	0%	1
SAST	0%	17%	50%	0%	33%	0%	6
Security Weaver	0%	0%	0%	100%	0%	0%	1
Mesaforte	0%	25%	75%	0%	0%	0%	4
CheckAud	14%	14%	57%	0%	14%	14%	7
XAMS	20%	20%	20%	20%	20%	20%	5
apm atlantis	22%	33%	33%	0%	11%	22%	9
GRC	0%	0%	22%	22%	56%	0%	18

Abbildung 4: Kosten pro Jahr pro Tool

Generell kann man zwei Preisklassen erkennen. Die preislich teureren Tools sind GRC und S.Siam. Weniger Kosten entstehen im Jahr mit den Tools DSR, SAST Security Weaver, Mesaforte, CheckAud und apm Atlantis. Eine Ausnahme ist hier XAMS. Das Tool der Firma XITING bewegt sich hier über beide Preissegmente.

Unterstützung des Rollenbaus und Berechtigungsmanagement

Der manuelle Rollenbau ist zeit- und somit kostspielig. Viele Unternehmen haben mit dem manuellen Rollenbau schlechte Erfahrungen gemacht und setzen aus diesem Grund ein 3rd Party Tool ein, das Ihnen diese Aufgabe erleichtert.

Wie gut fühlen Sie sich beim Rollenbau und Berechtigungsmanagement unterstützt?

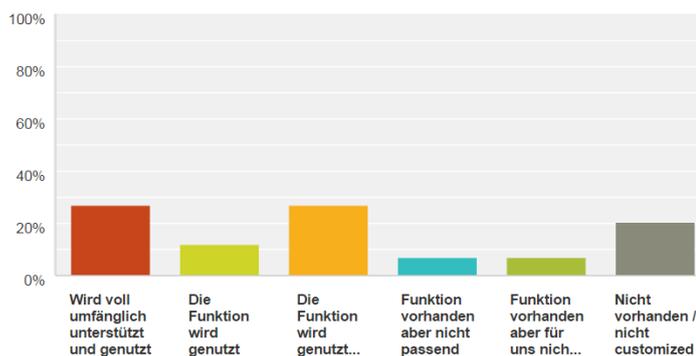


Abbildung 5: Unterstützung beim Rollenbau und Berechtigungsmanagement

27,03% der Teilnehmer geben an, dass Sie beim Rollenbau und Berechtigungsmanagement voll umfänglich unterstützt werden (Note 1). 12,16% geben dem Tool als Note eine 2 (Die Funktion wird genutzt). Die Funktion wird genutzt, aber einige Teile müssen manuell gemacht werden (Note 3) sagen 27.03%. Jeweils 6,76% geben an, dass die Funktion vorhanden, aber nicht passend ist bzw. dass die Funktion vorhanden, aber nicht sinnvoll nutzbar ist (Note 4 und Note 5). 29,27% der Teilnehmer geben an, dass diese Funktion nicht vorhanden oder nicht customized ist.

Tool	Zufriedenheit beim Rollenbau/ Berechtigungsmanagement						
	Note 1	Note 2	Note 3	Note 4	Note 5	Nicht vorhanden/ customized	Durchschnitts-note
DSR	20%	20%	0%	40%	20%	0%	3,20
S.Siam	0%	100%	0%	0%	0%	0%	2
SAST	40%	20%	0%	20%	0%	20%	2,8
Security Weaver	0%	0%	0%	0%	0%	100%	-
Mesaforte	33%	0%	33%	0%	0%	33%	2,05
CheckAud	0%	0%	67%	0%	0%	33%	4
XAMS	40%	20%	40%	0%	0%	0%	2
apm atlantis	38%	25%	25%	0%	12%	0%	2,25
GRC	25%	13%	19%	0%	19%	25%	3,5

Abbildung 6: Zufriedenheit beim Rollenbau und Berechtigungsmanagement pro Tool

Auswertung kritischer Berechtigungen

Kritische Berechtigungen sind Berechtigungen, die in sich kritisch sind, ohne dass die Art des Zugriffs auf diese Berechtigung schon definiert sein muss. (Technische Definition: Berechtigungsobjekt ohne Verbindung zu einer konkreten Transaktion). Ein Beispiel

Wie gut fühlen Sie sich bei der Auswertung kritischer Berechtigungen unterstützt?

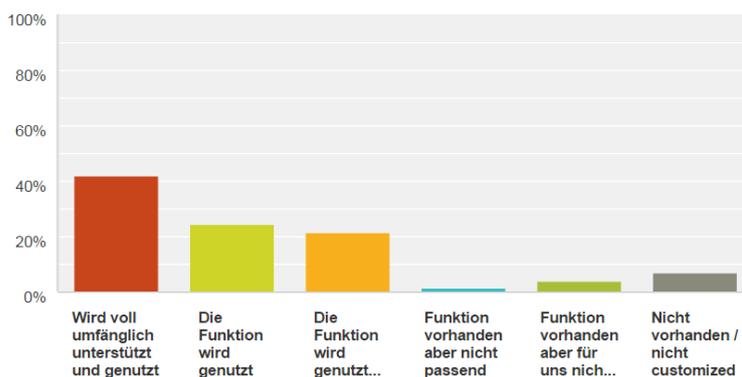


Abbildung 7: Auswertung kritischer Berechtigungen

ist das Debugging im Änderungsmodus. Es nützt keinem Unternehmen etwas, wenn nach der Einführung eines neuen Berechtigungskonzeptes trotzdem kritische Transaktionen (sei es nur durch Unwissenheit), wie z.B. die SE16 oder PFCG, vergeben werden. Diese Vergabe verwässert das Konzept und führt in häufigen Fällen zu einem baldigen Redesign. Diese Gefahr kann mit Hilfe von Tools stark reduziert werden. Die Auswertung kritischer Berechtigungen ist bei einigen Tools das Hauptfeature (siehe Frage 9.9). 41,89% der Teilnehmer geben ihrem Tool die Note 1 in Bezug auf die Auswertung von kritischen Berechtigungen. Note 2 und Note 3 liegen eng beieinander mit 24,32% und 21,62%. Die Noten 4 und 5 vergibt nahezu keiner (1,35% und 4,05%). 6,76% geben an, dass diese Funktion nicht vorhanden oder nicht customized ist.

Tool	Auswertung kritischer Berechtigungen pro Tool (gerundet)						
	Note 1	Note 2	Note 3	Note 4	Note 5	Nicht vorhanden / customized	Durchschnittsnote
DSR	100%	0%	0%	0%	0%	0%	1
S.Siam	0%	100%	0%	0%	0%	0%	2
SAST	80%	0%	20%	0%	0%	0%	1,4
Security Weaver	100%	0%	0%	0%	0%	0%	1
Mesaforte	67%	0%	0%	33%	0%	0%	2
CheckAud	50%	33%	17%	0%	0%	0%	1,67
XAMS	0%	40%	60%	0%	0%	0%	2,6
apm atlantis	25%	38%	38%	0%	0%	0%	2,13
GRC	38%	38%	19%	0%	0%	6%	2,06

Abbildung 8: Auswertung kritischer Berechtigungen pro Tool

Sie wollen die komplette Studie erwerben?

Melden Sie sich bei mir: funk@mindsquare.de

Oder erwerben Sie unser Fachwissen in Form der Marktvergleichsstudie direkt:

<http://studie-sap-berechtigungs-tools.de/>

<http://rz10.de>